IP Peer Review for Security

Freemon Johnson

GSFC Code 585

Phone: 301-286-1567

Email: Freemon.Johnson@gsfc.nasa.gov

Space IP Security Presentation

*This presentation will describe specific points of investigation of the IP Security Team's objectives in addition to the SOMO Technology contract support that will help to mitigate vulnerabilities, threats for using IP on a spacecraft for telemetry, tracking and command via the Internet.

* The goal is to leverage off of existing COT security solutions with commercial implementation of ***high*** valued assets e.g. Bank architectures

* ***All architecture, products, implementation examples shown are for conceptual purposes only!***

*The deliverable will be a handbook for recommendations that missions can adhere to depending on their method of operation, monetary value, mission classification and affiliation with NASA.

Risk

A risk is nothing more than a threat to which the system is vulnerable.

- Vulnerabilities and threats are then the focus of a Risk Assessment.
- To minimize risk one must either reduce the threat or the vulnerability to which a system can be subjected to.

Vulnerabilities

- All computers on a domain that have a point of entry or node to a gateway.
- All network devices that have remote configuration capabilities that are within a domain of a PI/FOT workstation.
- All computers that are susceptible to being operated by unauthorized personnel.
- All RF communication to and from a spacecraft.
- All computers that are running daemons and server software that is tied into the operating system.

Threats

- Chances to compromise a switch, router, firewall, etc.
- Chances to compromise daemon or server software running.
- Chances of an unauthorized personnel operating a command terminal e.g. ITOS.
- Chances of anyone radiating to a spacecraft with their own equipment for malicious purposes.
- Accidents do occur and other non-malicious attempts.

Mitigating Compromising Points of Entry

- Establish encrypted remote communication to all network equipment and devices.
- Install and configure firewall boxes, and proxies for each node between autonomous networks of operation.
- Send data continuously to keep the line of traffic active while in contact with the spacecraft. Prevents against *traffic profiling*. Schedules should not be publicized.
- Install any patches for flawed daemons and security applications.
- Use biometrics to validate the user issuing the command.

Note: **International CD&H vs Domestic determines allowable security implementations. Export Laws will vary as well as the security policies.**

Security Protocols

© **SSL/TLS** (Secure Socket Layer and Transport Layer Security) - TLS is SSL ver.3.0. (TCP only)

© **Triple DES** - 2 keys used for albeit algorithm.

AES - The successor to DES with better encryption algorithms.

© **IPSEC** - Transport mode or tunnel mode e.g. encrypt the IP datagram or protect the upper layer protocols. (TCP and UDP for packet by packet encryption)

GKMP (Group Key Management Protocol) - Shared, public, IKE, and PKI keys for multicast security.

RC4 - stream cipher encryption as opposed to block coding. It adds the output of a pseudo random number generator bit by bit to the sequential bits of a digitized plaintext.

© **RSA/DSS** - Public Key Encryption (good for non- repudiation). (Slow for packet by packet processing though)

© **PKI** (Public Key Infrastructures) - Servers and or device that store and distribute key information.

© **PPTP/L2TP** (Point to Point Tunneling Protocol) - IPSEC twin for Microsoft Windows operating systems.

Others: Blowfish, Twofish, X.509, GSAKMP, BEEP, IMDEF, SMI-XML, NGISec, etc.

© = *Commercially available and implemented.*

Security Applications

© **Kerberos** - Can replace FTP, Telnet, RLogin, RSH and RCP. Uses public key encryption and relies on a ticket server like IKE.

© **SSH** - Can replace FTP, Telnet, RLogin, RSH and RCP. Uses RSA and DSA for authentication, and all common encryption standards. Also uses public key encryption standards.

© **PGP** (Pretty Good Protection) - is Public Key Encryption with a compressed cipher block. Used primarily for email.

Syslog Reliable - Is a revised version of Syslog on POSIX based UNIX systems. It is designed to prevent against capture/replay, sequencing, gaps, and non-repudiation. Uses signature blocks with digital signatures e.g. DSA and RSA. Uses BEEP protocol for the transport layer.

© = Commercially available and implemented.

Security Hardware

-There are DSPs with "off-board" processing that can and are being utilized to handle encryption algorithms to relieve CPU cycles, memory, and processing time of the main processor.

- For the purposes of spacecraft, re-configurable FPGAs are being researched.

More info:

http://www.ece.wpi.edu/Research/crypt/research/index.html

Possible Phase V Security Architecture Overview

PI/FOT - Biometrics, digital signatures.

Many PI-to-spacecraft or vise versa or many spacecraft-to-spacecraft: GSAKMP (Group Secure Association Management Protocol) for multicast security.

PI/FOT Workstation - SSL, IPSEC, SSH ,etc.

PI Peripherals (e.g. Palm OS) - embedded Linux that is already extensible for open source security implementation.

RAS Terminal (Dial-Up) - PPTP

Open and Closed IONET - NGISec, Firewall, IPCHAINS, proxies, etc.

Direct-To-Spacecraft - Firewall at ground station gateway.

Spacecraft - embedded Linux that is extensible for all IETF security protocols and security applications that are in existence today and in the future.

Command - will have at a minimum, access control, assured usage, data integrity, confidentiality, and authentication controls implemented.

Telemetry - will have authentication at a minimum and all other attributes will depend on their method of operation, monetary value, mission classification and affiliation with NASA.

Sequence of Analysis